REMARKS

Claims 1 and 3-33 are currently pending in the subject application and are presently under consideration. Claims 1, 4-6, 10, 12-15, 17- 24, 26-30 and 32 have been amended as shown on pp. 2-7 of the Reply. Claims 3 and 25 are cancelled.

Favorable reconsideration of the subject patent application is respectfully requested in view of the comments and amendments herein.

I. Rejection of Claims 1, 5-7, 9, 10, 20, 23-25 and 27-29 Under 35 U.S.C. §103(a)

Claims 1, 5-7, 9, 10, 20, 23-25 and 27-29 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Spriggs, *et al.* (US 6,421,571) in view of Abraham (US 5,539,906). It is requested that this rejection be withdrawn for at least the following reasons. Spriggs, *et al.* and Abraham taken alone or in combination do not teach or suggest every element of the claimed invention, and further, one ordinarily skilled in the art could not combine these references to successfully implement the claimed invention.

> To reject claims in an application under §103, an examiner must establish a *prima facie* case of obviousness. A *prima facie* case of obviousness is established by a showing of three basic criteria. First, there ***must be some suggestion or motivation***, either in the references themselves or in the knowledge generally available to ***one of ordinary skill in the art, to modify the reference or to combine reference teachings***. Second there must be a ***reasonable expectation of success***. Finally, the prior art reference (or references when combined) ***must teach or suggest all the claim limitations***. *See* MPEP §706.02(j). The ***teaching or suggestion to make the claimed combination*** and the reasonable expectation of success ***must be found in the prior art and not based on the Applicant's disclosure***. *See In re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991) (emphasis added).

The claimed subject matter generally relates to a system that automates security in an industrial control environment by automatically creating security profiles for industrial automation devices in the environment and enforcing these profiles with respect to accessing entities. Such profiles may define different levels of access for various entities. In an industrial automation environment, efficient operation may depend upon rapid granting of access to low-level components to users not generally trusted with access to

high-level components. For example, repair of components may require access for outside contractors operating via the Internet. For regular users, prespecification of levels of access is often sufficient. By contrast, in these important cases, automation of security risk analysis is desirable.

As currently amended, independent claim 1 recites an automation security system, comprising: an asset component that defines an industrial automation device; an access component that defines a security attribute associated with the industrial automation device, the security attribute including a location attribute and a time attribute that grants access to the industrial automation device for a predetermined amount of time; and a ***security component that*** regulates access to the industrial automation device based upon the security attribute and ***includes an automated security assessment component.*** (emphasis added)

Spriggs *et al.* discloses a system that includes a unified display environment and a common database structure for protecting and managing industrial plant assets. (Col. 3, lns. 20-25). Spriggs *et al.* also discloses using a security manager module that provides configuration security settings for the system wherein the security is configured based on the logged-in user and certain tasks, such as editing set points or acknowledging events. (Col. 27 ln. 64 - Col. 28 ln. 1). Abraham discloses a data processing system for controlling data security in a data processing system. (Col 2, lns. 47-50). Further, Abraham discloses that user groups which access data are located at a plurality of locations, and a copy of selected database elements is associated with each location. (Col. 3, lns. 17-20). Abraham also discloses that access will be denied to a user based on the status of the data and the location of the user. (Col. 3, lns. 20-22). Moreover, Abraham discloses that a manufacturing engineer, for example, at a particular location can only access a copy of the design data which is associated with that particular location. (Col. 3, lns. 22-25).

However, neither Spriggs *et al.* nor Abraham teach, disclose or suggest that the decisions made on assigning levels of security to individual users as part of constructing the security attribute be an automated process. As pointed out by the Examiner, acting on these decisions by automated implementation of a security component is indeed described in prior art. However, in Examiner's references, these decisions are user-

specified. By contrast, Applicant claims automation of not merely implementation of the security component but also of the decisions as to security level that establish the security aspect underlying the security component. As such, Spriggs, *et al.* and Abraham, when taken alone or in combination, fail to teach or suggest every element of independent claim 1, and for at least the aforementioned reasons the rejection should be removed.

Amended independent claim 20 recites an automation security system, comprising: a server that manages a network interface between networked industrial automation devices and other devices attempting access to the networked industrial automation devices; and ***a security management module*** associated with the network interface that enforces an enterprise wide policy and that manages security threats directed to the networked industrial automation devices, the enterprise wide policy including a location attribute and a time attribute that limits access to the networked industrial automation devices to certain time periods, and ***utilizes the results of automated security threat analysis.*** (emphasis added)

Spriggs *et al.* discloses a system that includes a unified display environment and a common database structure for protecting and managing industrial plant assets. (Col. 3, lns. 20-25). Spriggs *et al.* also discloses the system is capable of correlating information from multiple sources that allows timely, operational decisions on machinery condition that consider both the machinery and the surrounding process conditions/constraints (Col 2, lns. 27-31).

However, Spriggs *et al.* is silent regarding an automated threat analysis system. By contrast, Applicant claims this novel feature, including in the system capacity for enabling the important innovation of allowing new users of low-level equipment rapid, on-line clearance through security features in order, for example, to have timely access to plant assets that require repair, maintenance or monitoring. Likewise, Abraham is also silent to such novel aspects. As such, Spriggs, *et al.* and Abraham, when taken alone or in combination, fail to teach or suggest every element of independent claim 20, and for at least the aforementioned reasons the rejection should be removed.

Amended independent claim 24 recites an automation security methodology, comprising electronically analyzing an industrial automation device; programmatically modeling the industrial automation device in accordance with network security

considerations, the network considerations include a location attribute and a time attribute that controls if and how long network access is granted to the industrial automation device; and automatically ***developing a security framework for an automation system based in part on*** the modeling of the industrial automation device, a network access type and ***at least one of a formal threat analysis, a vulnerability analysis, a factory topology mapping, or an attack tree analysis to determine whether access should be granted*** to the industrial automation device.

Spriggs *et al.* discloses providing configuration security settings for the system wherein the security is configured based on the logged-in user and certain tasks, such as editing set points or acknowledging events (Col. 27, ln. 64 through Col. 68, ln. 4). Additionally, Abraham discloses granting security access to users based on the status and location of the users (Col. 3, lns. 17-25).

However, Spriggs *et al* is silent regarding a method for automated process for determining whether access should be granted to the industrial automation device based on automated security risk analysis. By contrast, Applicant claims this novel feature, enabling the important innovation of allowing new users of low-level equipment rapid, on-line clearance through security features in order, for example, to have timely access to plant assets that require repair, maintenance or monitoring. Likewise, Abraham is also silent to such novel aspects. As such, Spriggs, *et al.* and Abraham, when taken alone or in combination, fail to teach or suggest every element of independent claim 20, and for at least the aforementioned reasons the rejection should be removed.

Amended independent claim 28 now recites an automated security system for an industrial control environment, comprising: means for defining one or more security attributes associated with at least one network request, the security attributes include at least one of: a location attribute, a time attribute, a role attribute, or an access type attribute; means for processing the one or more security attributes; ***means for automatically determining which network devices require security resources based on at least one of a formal threat analysis, a vulnerability analysis, a factory topology mapping, or an attack tree analysis***; and means for controlling access to at least one of a network device or the industrial automation component based in part on the one or more security attributes.

Spriggs *et al.* discloses a system wherein the security is configured based on the logged-in user (Col. 27, lns. 65-67). Abraham discloses granting security access to users based on status and locations of the users (Col. 3 lns. 17-25). Further, Abraham discloses a security level that can be based on granting access to different security groups. (Col. 7, lns. 1-5).

As depicted in the specification for the claimed subject matter, a security model can include asset and access based models having respective security attributes that describe the type of automation component to be accessed and the type of access permitted within the automation component such as a read and/or write access. (Pg. 6, lns. 7-12). Further, the specification for the claimed subject matter discloses that the security models can include role information or attributes relating to the users who attempt access (*e.g.,* Manager, Engineer, Maintenance) and can include a time-coded attribute limited entry to a device to a specified time. (Pg. 3, lns. 27-29 and Pg. 17, ln. 27).

Importantly, applicant claims that the system for granting access to system assets via a network is contingent upon function of the automated security risk analysis system. Spriggs et al. and Abraham are both silent with regard to this limitation of claim 28. As such, Spriggs, *et al.* and Abraham, when taken alone or in combination, fail to teach or suggest every element of independent claim 28, and for at least the aforementioned reasons the rejection should be removed.

Amended claim 29 recites a security schema for a factory automation system, comprising: a first data field that describes industrial automation devices; a second data field that describes security parameters for the industrial automation devices, ***the security parameters including*** a location attribute and a time attribute that enables access to the industrial automation devices for a specified time and ***attributes stemming from the results of automated security risk analysis***; and a schema that associates the first and second data fields, the schema employed to limit access to the industrial automation devices based upon the security parameters.

Spriggs teaches an action manager that configures security "based on the logged-in user and certain tasks, (Col. 27, lns. 66-67)" or "based on the particular

instrumentation (Col. 28, lns. 1-2)." Abraham further teaches granting security access to users based on status and location of users (Col. 3, lns. 17-25).

Applicant teaches that the security parameters for the schema are determined in an automated process. Spriggs *et al.* and Abraham are both silent as to this feature. As such, Spriggs, *et al.* and Abraham, when taken alone or in combination, fail to teach or suggest every element of independent claim 20, and for at least the aforementioned reasons the rejection should be removed.

As claims 5-7, 9 and 10 depend upon amended claim 1, claim 23 depends on amended claim 20, claim 25 and 27 depend on amended claim 24, and the independent claims should now stand in condition of allowance, the rejections of dependent claims are moot and they should also stand in a condition of allowance. In view of at least the foregoing, it is readily apparent that Spriggs *et al.* even in light of Abraham fails to teach, disclose or suggest each and every element recited in the subject claims. Therefore, the rejection of claims 1, 20, 24, 28, and 29 (and associated dependent claims 5-7, 9, 10, 23, 25, and 27) should be withdrawn.

II. Rejection of Claims 3, 4, 11-19, 21-22, 26 and 30-33 Under 35 U.S.C. §103(a)

Claims 3, 4, 11-19, 21-22, 26, and 30-33 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Spriggs *et al.* in view of Abraham and in further view of Le Saint (US 2004/0034774). It is respectfully requested that this rejection be withdrawn for at least the following reasons. Spriggs et al. and Le Saint, when taken alone or in combination, fail to teach or suggest all elements recited in the subject claims

Examiner states, "Spriggs does not specifically discuss the security component is based on at least one of a formal threat analysis, a vulnerabilty analysis, a factory topology mapping and an attack tree analysis…" Examiner states that these features are claimed in Le Saint and refers to paragraph 48. Le Saint claims a system for delegating security privileges between data processing units (paragraph 6). Security privileges are assigned via passing security tokens (paragraph 48). However, Le Saint is silent on the decision making process by which data processing units are allowed to receive security tokens.

The system for security risk assessment is now part of all independent claims as currently amended (previously in claim 3, which is cancelled). As such, Le Saint fails to make up for the aforementioned deficiencies with respect to amended claims 1, 20, 24, 28 and 29, from which claims 4, 11-19, 21-22, 26, and 30-33 depend. Accordingly, it is respectfully requested that the rejection of these claims be withdrawn.

CONCLUSION

The present application is believed to be in condition for allowance in view of the above comments. A prompt action to such end is earnestly solicited.

In the event any fees are due in connection with this document, the Commissioner is authorized to charge those fees to Deposit Account No. 50-1063 [ALBRP303USA].

Should the Examiner believe a telephone interview would be helpful to expedite favorable prosecution, the Examiner is invited to contact applicants' undersigned representative at the telephone number below.

Respectfully submitted,

AMIN, TUROCY & CALVIN, LLP

/Himanshu S. Amin/
Himanshu S. Amin
Reg. No. 40,894

AMIN, TUROCY & CALVIN, LLP
24TH Floor, National City Center
1900 E. 9TH Street
Cleveland, Ohio 44114
Telephone (216) 696-8730
Facsimile (216) 696-8731

HSA/AS